



# **GDPR Policy**

## **Vbrick Systems**

Revision 3

February 2, 2023

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 2 of 15**  
**Date: Feb 2, 2023**

Revision History

Version	Name	Date	Notes
Draft	Terry Medhurst	December 26 <sup>th</sup> , 2016	For executive review
0.1	Terry Medhurst	January 16 <sup>th</sup> 2018	Updates following review by external council (Venable)
1	Terry Medhurst	April 18 <sup>th</sup> 2018	
2	Terry Medhurst	June 13 <sup>th</sup> 2019	Policy review and update
3	Terry Medhurst	February 2 <sup>nd</sup> 2023	Policy review and update internally and by external counsel

Approvals

Name	Role	Date	Signature
Paul Sparta	CEO		Recorded via Paylocity
Kim Sysak	HR Director		
Michael McDonnell	Legal Counsel		

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 3 of 15**  
**Date: Feb 2, 2023**

## TABLE OF CONTENTS

- 1. INTRODUCTION .....4**
  - 1.1. OBJECTIVE ..... 4
  - 1.2. SCOPE..... 4
  - 1.3. DISTRIBUTION ..... 4
  - 1.4. REVIEW, UPDATE AND MAINTENANCE ..... 4
  - 1.5. EXCEPTIONS..... 4
  - 1.6. APPROACH ..... 4
- 2. GDPR AWARENESS PROGRAM .....6**
- 3. SYSTEM DOCUMENTATION.....7**
- 4. VBRICK PRIVACY POLICY .....8**
- 5. PROTECTING CUSTOMER DATA .....9**
- 6. DOCUMENTING USE OF CAPTURED DATA..... ERROR! BOOKMARK NOT DEFINED.**
- 7. CAPTURING CONSENT..... ERROR! BOOKMARK NOT DEFINED.**
- 8. SUBJECT ACCESS REQUESTS .....12**
- 9. RIGHT TO BE FORGOTTEN .....13**
- 10. DATA BREACH NOTIFICATIONS .....14**
- 11. VBRICK DATA PROTECTION OFFICER .....15**

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 4 of 15**  
**Date: Feb 2, 2023**

## 1. INTRODUCTION

### 1.1. Objective

The objective of this policy is to describe the approach adopted by Vbrick Systems to EU General Data Protection Regulation ("GDPR") compliance.

Vbrick has data privacy and data protection obligations under the GDPR whenever Vbrick processes EU Personal Data as a "processor" or "controller." When Vbrick processes EU Personal Data on behalf of its customers as a "processor," our GDPR obligations will stem primarily via contract. When Vbrick processes EU Personal Data directly from individuals as a "controller," we will have obligations imposed on us by law.

This GDPR Policy, including any supporting GDPR Standards and Procedures, memorializes these obligations.

### 1.2. Scope

The scope of this policy applies to all Vbrick internal and customer facing systems that may contain personal data that is subject to the GDPR ("EU Personal Data").

### 1.3. Distribution

This document is classified Proprietary and Confidential. It must be disseminated to all relevant personnel. It is releasable to customers, vendors, business partners, individuals or organization that have a signed Non-Disclosure Agreement on file and have a reasonable business need for the information. Requests for distribution of this document should be directed to the CIO.

### 1.4. Review, Update and Maintenance

The GDPR Policy, including any supporting GDPR Standards and Procedures, are considered living documents. These documents are subject to changes and modification necessary. All documents shall be reviewed on at least an annual basis and the review must consider changes to laws, guidance issued by government authorities, and the risk environment over the past year.

### 1.5. Exceptions

Vbrick allows for exceptions to the GDPR Policy as well as GDPR Standards and Procedures in specific circumstances where mitigating controls are implemented to reduce risk. Exceptions are approved by the Information Systems Executive Steering Committee and are memorialized to file.

Exceptions are deviations from the identified guidelines and are granted with the expectation that the requesting party will expeditiously devise and implement a solution that allows for return to normal operations. All exception requests that have been granted must be reviewed annually or when the circumstances that led to the exception have changed.

### 1.6. Approach

Vbrick has adopted the following approach for addressing GDPR compliance that is described within this GDPR Policy:

1. GDPR awareness and training program
2. Documentation of systems containing EU Personal Data
3. Communication of privacy related information
4. Protecting customer data
5. Collecting and Handling EU Personal Data

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 5 of 15</b> <b>Date: Feb 2, 2023</b>

6. Processing subject access, portability, and correction requests
7. Processing applicable "right to be forgotten" and "right to restrict processing" requests
8. Data breach notifications
9. Designated Data Protection Officer

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 6 of 15**  
**Date: Feb 2, 2023**

## 2. GDPR Awareness Program

The Vbrick GDPR awareness program operates at two levels:

1. **Company-wide GDPR awareness** – This consists of annual privacy training that includes the principles of the GDPR and applicable privacy regulations for other countries where Vbrick does business.
2. **GDPR for information System Owners** – This is a more detailed awareness program to communicate the specific roles and responsibilities for information system owners whose systems and applications may contain data that is subject to GDPR. Information system owners are responsible for processing requests related to individual’s rights under GDPR. System Owners are required to complete formal GDPR training that has been made available [here](#). The Vbrick CIO is responsible for ensuring compliance with GDPR training.

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 7 of 15</b> <b>Date: Feb 2, 2023</b>

### 3. System Documentation

Vbrick information systems are documented in an asset tracking spreadsheet. The spreadsheet captures a range of system information including the Information Owner, Information Custodian, Information Classification, Application Criticality and whether the system contains EU Personal Data.

Where a system has been identified as potentially capturing EU Personal Data, additional information is captured including:

1. Whether Vbrick is acting as a data controller or data processor
2. Whether sub-processor(s) are involved in processing the EU Personal Data
3. The personal data elements that are captured
4. The reason for capturing the personal data elements
5. The lawful basis for processing
6. How long the personal data is retained
7. How consent is captured
8. How subject access requests are processed
9. The physical location where EU Personal Data is stored
10. Any third parties to whom EU Personal Data is disclosed

The asset tracking spreadsheet that list systems subject to the GDPR can be found [here](#). Documentation that details points 1 thru 10 shown above can be found [here](#).

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 8 of 15**  
**Date: Feb 2, 2023**

#### 4. Vbrick Privacy Policy

The Vbrick privacy policy and GDPR Policy has been updated to reflect the requirements of the GDPR and Vbrick has determined that the policy shall apply to all customers, partners and employees worldwide who process EU Personal Data. The policy and any future updates are sent to all employees (via Paylocity) and contractors (via email) for formal acknowledgement.



	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 9 of 15**  
**Date: Feb 2, 2023**

## 5. Protecting Customer Data

VBrick shall ensure appropriate controls are implemented to adequately protect customer, partner and employee EU Personal Data. Customer, partner and employee EU Personal Data shall be encrypted in motion and at rest. Where legacy systems do not have the capability to provide this level of protection or cannot be upgraded to do so, a risk assessment must be performed and, if applicable, an exception to policy documented.

Where sub-processors have been identified that process EU Personal Data on behalf of Vbrick, a data processing amendment must be sent to all identified vendors for execution or the vendor's own DPA must be reviewed for adequacy. Details of the Vbrick DPA can be found [here](#).

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 10 of 15**  
**Date: Feb 2, 2023**

## 6. Collecting and Handling EU Personal Data

### 6.1. Collecting EU Personal Data

Before Vbrick collects EU Personal Data directly from data subjects, the capturing system shall clearly explain to the data subject how the EU Personal Data captured is used by Vbrick and to whom Vbrick discloses that data. This explanation can take the form of the Vbrick Privacy Policy. The capturing system must also require that the user positively consents to that use of EU Personal Data where consent is required by law. The method by which consent shall be recorded will vary by system. Data subjects have the right and ability to revoke this consent at any time.

Documentation that how consent is captured for each in scope system can be found [here](#).

In other instances, EU Personal Data may be processed pursuant to means other than consent, such as because it is necessary to fulfill the terms of a contract to which the user is subject. In those cases, Vbrick shall memorialize the lawful basis of processing EU Personal Data.

### 6.2. Handling EU Personal Data

Vbrick will follow the procedures described in the Data Protection Policy to ensure proper handling of EU Personal Data.

For avoidance of doubt, when handling customer EU Personal Data, the following obligations will also apply:

- Vbrick will only act on the controller’s documented instructions.
- Vbrick will impose confidentiality obligations on all personnel with access to EU Personal Data.
- Vbrick will assist customers in honoring data rights requests when Vbrick has processed data about the data subject for the customer.
- Vbrick will follow the controller’s instructions regarding the return or destruction of EU Personal Data at the termination of the Agreement.

### 6.3. Privacy Impact Assessments

Vbrick will conduct a privacy impact assessment to determine the benefits and risks of processing certain types of data before Vbrick processes EU Personal Data that presents a high risk to the rights and freedoms of natural persons. Vbrick will use reasonable efforts to assist customers in completing the same upon reasonable request.

### 6.4. Transfer Impact Assessment

When Vbrick transfers EU Personal data to a non-adequacy approved third country, Vbrick will conduct a transfer impact assessment to assess the laws and practices of the non-adequacy approved third country to determine the sufficiency of the third country’s data protection laws and the risk of access by the foreign government. Vbrick will use reasonable efforts to assist customers in completing the same upon reasonable request.

### 6.5. Third-Party Requests for EU Personal Data

If a third party requests customer EU Personal Data held by Vbrick, Vbrick will notify the customer of such a request before disclosing EU Personal Data. When law enforcement requests customer EU Personal Data held by Vbrick, Vbrick will not disclose customer EU Personal Data unless compelled to do so by a legally valid and binding order. Unless legally prohibited from doing so, Vbrick will notify the customer of such a request and refer law enforcement to the customer to issue such a request.

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 11 of 15</b> <b>Date: Feb 2, 2023</b>

	Policy	IS-POL-02
	<b>GDPR Policy</b>	

**Rev: 3**  
**Page: 12 of 15**  
**Date: Feb 2, 2023**

## 7. Subject Access, Portability, and Correction Requests

The information owner of each system that holds EU Personal Data shall be responsible for defining the process to extract the EU Personal Data held on the data subject upon reasonable request to satisfy both access and data portability requests. The information owner is also responsible for defining the process for correcting EU Personal Data held on the data subject.

Documentation that explains how data subject requests are processed can be found [here](#).

Data subject requests can be submitted via Vbrick customer support (contact details are prominently displayed on the Vbrick corporate website) or by emailing requests to [privacy@vbrick.com](mailto:privacy@vbrick.com).

Subject to appropriate verification of the requestor, the information subject to access or data portability request shall be made available in a human readable format determined by Vbrick.

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 13 of 15</b> <b>Date: Feb 2, 2023</b>

## 8. Rights to Be Forgotten and to Restrict Processing

The information owner of each system that holds EU Personal Data shall be responsible for defining the process to purge EU Personal Data held about the data subject upon reasonable request. The information owner of each system is also responsible for defining the process to restrict processing EU Personal Data about a data subject upon verified request. Documentation that explains how data subject requests are processed can be found [here](#).

However, any such request shall not impinge upon any obligation to comply requests from law enforcement or adversely impact the operation of the system where that data is stored.

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 14 of 15</b> <b>Date: Feb 2, 2023</b>

## 9. Data Breach Notifications

Vbrick internal information security processes are aligned with GDPR data breach notification requirements. Details of Vbrick data breach response procedures can be found [here](#). For customer and Partner EU Personal Data Vbrick maintains a data breach contact name in our Customer Relationship Management (CRM) System.

Vbrick Human Resources maintains contact information for employees to be notified in the event of a data breach.

	Policy	IS-POL-02
	<b>GDPR Policy</b>	<b>Rev: 3</b> <b>Page: 15 of 15</b> <b>Date: Feb 2, 2023</b>

## 10. Vbrick Data Protection Officer

Based on the scope of the personal information captured by Vbrick and its permitted use, Vbrick has appointed a named Data Protection Officer. GDPR responsibilities, policies and procedures are reviewed by such Data Protection Officer and that person will serve as main point of contact for GDPR related initiatives.